ABSTRACT

A parameter generation apparatus for generating parameters causing no decryption error for an NTRU cryptosystem so that an encrypted communication can be carried out between an encryption apparatus and a decryption apparatus in a secure and reliable manner. The parameter generation apparatus includes: a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, the error condition information indicating a condition for causing no decryption error; and an output parameter generation unit operable to generate an output parameter that does not cause any decryption errors, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters.